Confirmation No. 4003

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	PESSOLANO	Examiner:	King, John B.
Serial No.:	10/553,790	Group Art Unit:	2435
Filed:	October 19, 2005	Docket No.:	NL030397US1 (NXPS.589PA)
Title:	ELECTRONIC CIRCUIT DEVICE FOR CRYPTOGRAPHIC APPLICATIONS		

APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Customer No.
65913

Dear Sir:

This Appeal Brief is submitted pursuant to 37 C.F.R. §41.37, in support of the Notice of Appeal filed June 24, 2010 and in response to the rejections of claims 1-8 and 10-14 as set forth in the Final Office Action dated April 1, 2010.

Please charge Deposit Account No. 50-4019 (NL030397US1) $540.00 for filing this brief in support of an appeal as set forth in 37 C.F.R. §1.17(c). If necessary, authority is given to charge/credit Deposit Account 50-4019 additional fees/overages in support of this filing.

I. Real Party In Interest

The real party in interest is NXP Semiconductors. The application is presently assigned of record, at reel/frame nos. 019719/0843 to NXP, B.V., headquartered in Eindhoven, the Netherlands.

II. Related Appeals and Interferences

While Appellant is aware of other pending applications owned by the above-identified Assignee, Appellant is unaware of any related appeals, interferences or judicial proceedings that would have a bearing on the Board's decision in the instant appeal.

III. Status of Claims

Claims 1-8 and 10-14 stand rejected and are presented for appeal. Claim 9 has been cancelled. A complete listing of the claims under appeal is provided in an Appendix to this Brief.

IV. Status of Amendments

No amendments have been filed subsequent to the Final Office Action dated April 1, 2010.

V. Summary of Claimed Subject Matter

As required by 37 C.F.R. § 41.37(c)(1)(v), a concise explanation of the subject matter defined in the independent claims involved in the appeal is provided herein. Appellant notes that representative subject matter is identified for these claims; however, the abundance of supporting subject matter in the application prohibits identifying all textual and diagrammatic references to each claimed recitation. Appellant thus submits that other application subject matter, which supports the claims but is not specifically identified above, may be found elsewhere in the application. Appellant further notes that this summary does not provide an exhaustive or exclusive view of the present subject matter, and Appellant refers to the appended claims and their legal equivalents for a complete statement of the invention.

Commensurate with independent claim 1, an example embodiment of the present invention is directed to an electronic circuit device for executing operations dependent on

secret information (*see, e.g.*, page 2:20-23). The electronic circuit device includes power supply connections (*see, e.g.*, Figure 1, Vdd and Vss). The device also includes a processing unit including a plurality of processing circuits for use in execution of respective parts of the operations dependent on the secret information (*see, e.g.*, Figure 1 references 102a and 102b). The processing circuits are fed from the power supply connections (*see, e.g., id.*). An activity monitor circuit is coupled to receive processing signals (*see, e.g.*, Figure 1, references 12a and 12b). Each of the pairs of processing signals includes an input signal and an output signal of one of the processing circuits (*see, e.g.*, Figure 1, reference 12a, and page 4:7-8). The activity monitor circuit is arranged to derive activity information from each pair of processing signals (*see, e.g.,* page 4:14-16). The activity information is indicative of whether each of the processing circuits generates a logic level transition (*see, e.g.*, page 4:17-18). The activity monitor is arranged to derive from the activity information a combined activity signal indicative of a sum of power supply currents that will be consumed by the processing circuits dependent on the processing signals (*see, e.g.*, page 4:18-29). A current drawing circuit is connected to the power supply connections and controlled by the activity monitor circuit (*see, e.g.*, Figure 1, reference 18) to draw a cloaking current controlled by the combined activity signal, so that power supply current variations dependent on the secret information are cloaked in a combination of the cloaking current and current drawn by the processing circuits (*see, e.g.*, page 5:1-5).

Commensurate with independent claim 7, an example embodiment of the present invention is directed to a method of executing operations depending on secret information in an electronic circuit (*see, e.g.*, page 2:20-23). The method includes supply power supply current to processing circuits (*see, e.g.*, Figure 1, Vdd and Vss). The method further includes executing respective parts of operations that are dependent on the secret information using the processing circuits. Pairs of processing signals coming into and out of respective ones of the processing circuits are received, and each of the pairs of processing signals includes an input signal and an output signal of one of the processing circuits (*see, e.g.*, Figure 1, references 12a and 12b, and page 4:7-8). Activity information is derived from each pair of processing signals and the activity information is indicative of whether each of the processing circuits generates a logic level transition (*see, e.g.*, page 4:14-18). A combined

activity signal indicative of a sum of the power supply currents that will be consumed by the processing circuits dependent on the processing signals is derived from the activity information (*see, e.g.*, page 2: 26-29). The method further includes drawing a cloaking current controlled by the combined activity signal (*see, e.g.*, page 5:1-5), and combining the cloaking current with current drawn by the processing circuits so that power supply current variations dependent on the secret information are cloaked in the combination of the cloaking current and current drawn by the processing circuits (*see. e.g.*, page 3:4-26).

VI. Grounds of Rejection to be Reviewed Upon Appeal

The grounds of rejection to be reviewed on appeal are as follows:

A. Claims 1 and 7 stand rejected under 35 U.S.C. § 112(2).
B. Claims 1, 5-8 and 10-14 stand rejected under 35 U.S.C. § 103(a) over Thuringer (U.S. Patent No. 6,498,404) in view of Odinak (U.S. Patent No. 6,419,159) and further in view of AAPA.
C. Claims 2-4 stand rejected under 35 U.S.C. § 103(a) over the '404 and '159 references and AAPA, and further in view of the Patterson reference ("Computer Architecture: A Quantitative Approach", pp. 134-135, 1995).

VII. Argument

A. The § 112(2) Rejection Of Claims 1 And 7 Is Improper.

The § 112(2) rejection is improper because it fails to establish that one of skill in the art would be incapable of understanding the claimed invention, and instead relies upon an assertion regarding Appellant's statements, which are not a proper basis for a § 112(2) rejection. *See* M.P.E.P. §§ 706.03(d) and 2173 *et. seq.* Specifically, the Office Action improperly asserts that Appellant's seemingly clear and unambiguous claim term is unclear and ambiguous if the claim term would be read in the context of (or relative to) a circuit that would somehow be arranged as a feedback loop system. As Appellant's claims do not even include the term "feedback," the basis for the § 112(2) rejection, rather than Appellant's claims, would seem to be the item lacking in clarity.

At issue is a claim term involving two sets (or pairs) of signals, where each signal pair includes an input signal and an output signal from one of the claimed circuits. For example, claim 1 is directed to an activity monitor and a processing circuit that are

respectively claimed separately and distinctly from each other. The processing circuit is claimed as having the input and output signals provided to the activity monitor. The claim term reads in pertinent part: "each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits". The record is clear that the activity monitor is not the same (processing) circuit from which the input and output signals originate, and that the claimed invention does not expressly mention a feedback loop. Thus, one skilled in the art would not become confused and for some reason, as asserted by the Examiner, assume or understand the claim to be including a feedback loop for the processing circuit.

Further, one of skill in the art would understand this limitation ("each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits") to be clear based on the plain meaning of the words within the limitation. Specifically, a pair of signals, defined previously in the claim as received by an activity monitor, includes an input signal from a processing circuit and an output signal from the same processing circuit. The Examiner has failed to establish that the words in the claim limitations apply to anything other than their plain meaning.[1] Accordingly, the Examiner has failed to present a proper § 112(2) rejection and Appellant requests the rejection be overturned.

The § 112(2) rejection is further improper because the Office Action has failed to establish that one of skill in the art would be incapable of understanding "what is claimed when the claim is read in light of the specification," contrary to the requirements of § 112(2) and M.P.E.P. § 2173.02. Appellant submits that one of skill in the art would understand the claim limitations regarding "pairs of processing signals including an input signal and an output signal of one of the processing circuits," in view of the claims as a whole and the specification. By way of example, Appellant refers to Figure 1 (reproduced below) as an embodiment that may be applicable to the claim limitations at issue. The discussion of

[1] The Examiner attempts to support the rejection by referencing and asserting out of context a previously-presented argument from an underlying Office Action Response. The specifics (and propriety) thereof need not be addressed further because the patent law would clearly reject any such position that an argument by an applicant could somehow override the patent law and rules on interpreting claims based on their plain meaning and the specification. *See, e.g.,* M.P.E.P. §§ 706.03(d), 2173.02, 2111.

Figure 1 in the specification discloses circuits 12a and 12b as activity detection circuits, and circuits 102 and 106 as processing circuits. Focusing on the relationship between circuits 12a and 102, processing circuit 102 has an input 110 and an output 112. The specification discloses "input 110 and output 112 of a first processing circuit are coupled to the inputs of a first activity detection circuit 12a." page 4, lines 7-8 of specification. Accordingly, an activity monitor (12a) receives a pair of processing signals that includes an input signal of a processing circuit and an output signal of the same processing circuit. These examples clearly support Appellant's assertions that one of skill in the art would understand the above-referenced claim limitations, in view of the specification or otherwise.

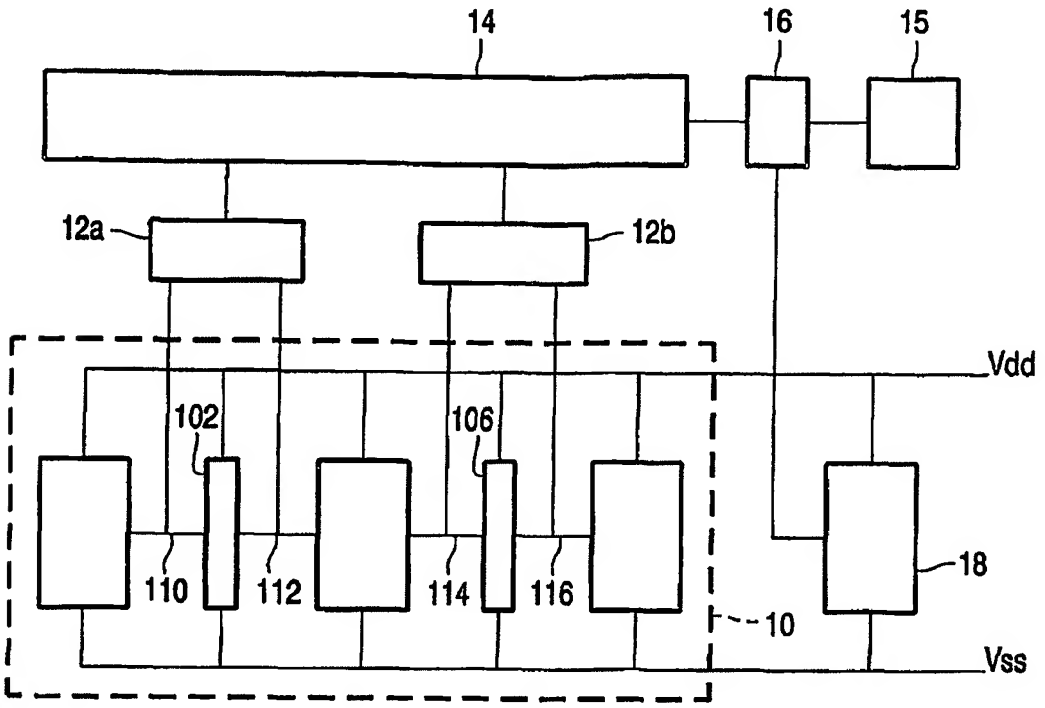


FIG. 1

Moreover, Appellant submits one of skill in the art would understand the plain meaning of the limitation in question in accordance with M.P.E.P. § 2173.02, which explains that "the examiner must consider the claim as a whole to determine whether the claim apprises one of ordinary skill in the art of its scope and, therefore, serves the notice function required by 35 U.S.C. 112, second paragraph." The Examiner's assertion that it is unclear whether the limitation "means that the processing circuit contains an input and output signal

if the circuit is arranged as a feedback loop system" (page 4 of Office Action dated April 1, 2010) fails to consider the claim "as a whole". Specifically, as a whole claim 1 includes an activity monitor, which is claimed separately and distinctly from the processing circuit that the claim associates with the input and output signals provided to the activity monitor.

In view of the above, the Office Action has failed to establish that the claim limitations referenced in the § 112(2) rejection are indefinite, and Appellant requests the § 112(2) rejection of claims 1 and 7 be reversed.

B. The § 103(a) Rejection Of Claims 1, 5-8 And 10-14 Is Improper.

1. The Proposed Combination Of References Lacks Correspondence.

The Examiner's asserted hypothetical combination of references lacks correspondence to certain aspects of the claimed invention including, for example, those directed to an activity monitor circuit that receives pairs of processing signals, with "each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits." In short, the asserted input signal (per the proposed combination) is instead a feedback signal that fails to correspond to the claimed approach in which the claimed input is drawn from a different circuit. More specifically, in attempting to assert correspondence to these aspects, the Office Action relies on AAPA as teaching a circuit including a feedback loop, which (as understood by one of skill in the art) involves providing an output of the circuit as a feedback input of that same circuit. The claim language, in contrast, requires that the input and output signals of a processing circuit be used as the input of a separate circuit, such as the activity monitoring circuit of claim 1. Accordingly, the input of a circuit in the AAPA that includes a feedback loop does not correspond to the pair of processing signals claimed. As the Examiner has not asserted any of the other references as teaching such aspects, and the references do not appear to Appellant to teach such aspects, the asserted hypothetical combination lacks correspondence.

The asserted hypothetical combination of references further lacks correspondence to certain aspects of the claimed invention directed to deriving activity information from the pair of processing signals that indicates whether the processing circuit generates a logic level transition. In attempting to assert AAPA to modify the '404 reference, the Examiner

acknowledges that the '404 reference does not teach activity information derived from a pair of processing signals as claimed. The Examiner cites the AAPA as teaching limitations directed to monitoring the logic level changes of the circuit based on the pairs of processing signals. However, the asserted portions of Appellant's specification (AAPA) discussing the asserted feedback loop disclose its purpose as keeping the power supply current constant, and thus do not correspond as asserted.

More specifically, paragraphs 0003 and 0004 of Appellant's published application (the cited AAPA) discuss WO 00/026746, which is the parent application of the asserted '404 reference, which does not include an activity monitor as claimed. The '404 reference includes two AND gates, neither of which receives a pair of signals that include an input and an output from a processing circuit. Because the AND gates do not receive the proper inputs, they cannot derive activity information from the claimed pair of processing signals. It appears that AND gate 8 is being asserted as the activity monitor circuit while AND gate 5 is the processing circuit. The AND gate 8, however, cannot determine when a transition has occurred in the output of AND gate 5. The AND gate 5 only provides an output of 1 when both inputs are 1. A transition in logic from 0 to 1 only occurs when both inputs are changed to 1, and a transition from 1 to 0 occurs when either or both of the inputs change from 1 to 0. The AND gate 8, however, receives an input that has been inverted. Because of the inversion "AND-gate 8 switches to '1' when the inputs of the first AND gate are all of logic level '0', [and] it cannot be recognized from outside if switching occurs when all the inputs of the first AND-gate 5 are set to '0' or set to '1'." Col. 2:49-53 of the '404 reference. This also means that when the inputs to the AND gate 5 are any other combination (0 and 1, 1 and 0, or 1 and 1) the output of AND gate 8 is 0. Accordingly, there is not necessarily a change in state for AND gate 8 when a change in state from 0 to 1 occurs for AND gate 5. Therefore, AND gate 8 does not correspond to the claimed activity monitor (claim 1) or deriving activity information from the pair of processor signals (claims 1 and 7).

Moreover, the proposed combination of the '404 reference and the '159 reference does not correspond to aspects of the claimed invention directed to separate current drawing and activity monitoring circuits, with the current drawing circuit being controlled by the activity monitor circuit based on a combined activity signal derived by the activity monitor.

The addition of the AAPA, which is primarily duplicative of the '404 reference, does not fix this lack of correspondence. The rejections appear to be based primarily on the Examiner's misunderstanding of the operation of the cited embodiment of the '404 reference, in continuing to rely upon the load circuit discussed in Col. 1:28-38 of the '404 reference as allegedly corresponding to Appellant's current drawing circuit. However, this load circuit is in fact the complementary gates (*e.g.*, AND gate 8 of Fig. 2), which the Office Action alleges as corresponding to Appellant's activity monitor. *See, e.g.*, Col. 1:45-52 and Col. 2:39-57. The current drawing circuit cannot be controlled by the activity monitor circuit if it is also the activity monitor circuit. Accordingly, the cited load circuit of the '404 reference does not correspond to Appellant's current drawing circuit as suggested in the Office Action. Appellant also notes that the complementary gates of the '404 reference function independently from one another and, as such, the Office Action has failed to establish that these complementary gates necessarily derive a combined activity signal indicative of a sum of power supply currents consumed by multiple processing circuits, as in Appellant's claimed activity monitor circuit.

Accordingly, the asserted hypothetical embodiment lacks correspondence. Therefore, the § 103(a) rejection of claims 1, 5-8 and 10-14 lacks correspondence and Appellant requests the rejection be reversed.

2. The Examiner Fails To Provide A Valid Reason For The Asserted Hypothetical Combination.

Consistent with M.P.E.P. § 2143.01 and relevant case law, a § 103 rejection must provide evidence of motivation where a proposed combination of references would modify a primary reference. *See, e.g., See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (U.S. 2007). ("A patent composed of several elements is not proved obvious merely by demonstrating that each element was, independently, known in the prior art."). As applicable here, the Examiner's asserted hypothetical combination includes two modifications to the primary '404 reference, the first by the '159 reference and the second by AAPA. In both instances the asserted motivation for the modification is to increase the security of the system. However, the combination of the references for this purpose makes no logical sense

as the alleged modifications cannot be effected for a single resulting embodiment. Specifically, the '404 reference teaches using a constant power consumption to disguise the actual power consumed by the data carrier during security-relevant operations. *See, e.g.*, Col. 1:45-65. The AAPA also teaches that the feedback loop is used to "keep the power supply current constant." In contrast the '159 reference teaches the use of randomness in the current consumption to disguise the actual power consumption. Because the asserted enhanced security of the '159 reference and the AAPA reference come from two features (random current consumption and constant current consumption) that cannot be present at the same time, the asserted motivations result in a hypothetical combination that can logically only include one of the two modifications.

The § 103 rejection is also improper because the Examiner has failed to present evidence that the modification of the '404 reference would "increase the security of the system" relative to the unmodified '404 reference which already disguises the actual power consumed by the data carrier during security-relevant operations using complementary logic to achieve a constant power consumption. As such, the Examiner's proposed modification involves adding redundant circuitry to the '404 reference without any perceived benefit.

In responding to Appellant's previous arguments regarding the combination of the '404 reference and the '159 reference, the Office Action asserts that the two references teach different ways to mask the power supply fluctuations, and therefore it would be obvious to replace one with the other. This assertion ignores the technical difficulties of modifying the '404 reference. More specifically, the proposed combination involves extensively modifying the '404 reference to somehow implement the random current drawing circuitry 40 of the '159 reference. Accordingly, the Examiner's assertion of such a vague "articulated reasoning" (*e.g.,* to "increase the security of the system") in support of the modification is insufficient, particularly in view of the fact that the Office Action fails to present any evidence that the proposed combination would "increase the security of the system" relative to the unmodified '404 reference. *KSR* and M.P.E.P. § 2141 make it clear that such assertions are inapplicable where the operation of one of the references is modified. *See, e.g., KSR* 550 U.S. at 417. For example, according to M.P.E.P. § 2141, Applicant can rebut such assertions of obviousness simply by showing that "the elements in combination do not merely perform the function that

each element performs separately." This is also consistent with various parts of *KSR*, which repeatedly refer to combined teachings in which the cited references are not modified in their operation. In this instance at least one of the elements from either the '159 reference or the AAPA is not merely performing the function that the element performed separately. This must be the case because the '159 reference results in a random current value while the AAPA results in a constant current value. These two states are mutually exclusive. Accordingly, the Examiner has failed to present a *prima facie* case of obviousness and the § 103(a) rejection of claims 1, 5-8, and 10-14 should be reversed.

C. The § 103(a) Rejection Of Claims 2-4 Is Improper.

1. The Proposed Combination Of References Lacks Correspondence.

The Examiner's asserted hypothetical combination of references lacks correspondence to aspects of the claimed invention as discussed above in Section B(1) regarding the rejection of claim 1, from which claims 2-4 depend. The rejection of claims 2-4 further add the Patterson reference to the hypothetical combination proposed in rejecting claim 1, but nothing in the Patterson reference overcomes the lack of correspondence discussed above in Section B(1). For example, the asserted hypothetical combination of references lacks correspondence to aspects of the claimed invention directed to an activity monitor circuit that receives pairs of processing signals, "each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits." The Office Action relies on AAPA as teaching a feedback loop. However, one of skill in the art would understand a circuit with a feedback loop to provide the output of a circuit as one of the inputs of that same circuit. The claim language, in contrast, requires that the input and output signals of a processing circuit be used as the input of a separate circuit, the activity monitoring circuit. Accordingly, the input of a circuit in the AAPA that includes a feedback loop does not correspond to the pair of processing signals received by the activity monitor circuit claimed.

Further, the Patterson reference does not appear to teach limitations directed to registers having an input and output signal that are provided as input to an activity monitor. Instead, the "register" as alleged in the Office Action has been asserted as having a pair of

inputs and a pair of outputs. This however, does not correspond to limitations directed to a pair of processing signals that include an input and an output signal from a processing circuit. Accordingly, none the other asserted prior art references, including the additionally asserted Patterson reference, appear to teach the pair of processing signals claimed. Therefore, the asserted hypothetical combination lacks correspondence.

The Patterson reference further does not overcome the lack of correspondence to certain aspects of the claimed invention directed to activity information derived from the pair of processing signals. The Patterson reference is asserted to teach a clock and a pipelined data-path, not the claimed activity monitor. In attempting to assert AAPA to modify the '404 reference the Examiner acknowledges that the '404 reference does not teach activity information derived from a pair of processing signals as claimed. The Examiner cites the AAPA as teaching monitoring the logic level changes of the circuit based on the pairs of processing signals. However, the asserted portions of Appellant's specification discussing the asserted feedback loop discloses the purpose of the feedback loop as keeping the power supply current constant.

For at least these reasons, as well as the reasons outlined above discussing independent claim 1, from which claims 2-4 depend, the asserted hypothetical combination of references lacks correspondence to the claimed invention. Accordingly, Appellant requests the § 103(a) rejection of claims 2-4 be reversed.

2. The § 103(a) Rejection Of Claims 2-4 Is Improper For Lack Of A Proper Reason To Combine The References.

The Examiner's hypothetical combination of references includes the combination of references asserted for independent claim 1, from which claims 2-4 depend. Accordingly, the § 103(a) rejection of claims 2-4 is improper for at least the reasons discussed above in section B(2). Moreover, the rejection of claims 2-4 as further involving the Patterson reference fails to provide evidence of motivation, consistent with M.P.E.P. § 2143.01 and relevant case law, which require that a § 103 rejection provide evidence of motivation where a proposed combination of references would modify a primary reference. *See, e.g., See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (U.S. 2007). ("A patent composed of several elements is not

proved obvious merely by demonstrating that each element was, independently, known in the prior art.").

As applicable here, the Examiner's asserted hypothetical combination includes multiple modifications to the primary '404 reference, the first by the '159 reference, the second by AAPA, and the third by the Patterson reference. In the first two instances the asserted motivation for the modification is to increase the security of the system. However, the combination of the references for this purpose makes no logical sense. Specifically, the '404 reference teaches using a constant power consumption to disguise the actual power consumed by the data carrier during security-relevant operations. *See, e.g.*, Col. 1:45-65. In contrast, the '159 reference teaches the use of randomness in the current consumption to disguise the actual power consumption. The AAPA teaches that the feedback loop is used to "keep the power supply current constant." Because the asserted enhanced security of the '159 reference and the AAPA reference come from two features that cannot be present at the same time, the asserted motivations result in a hypothetical combination that can logically only include one of the two modifications. Moreover, the Examiner has failed to present evidence that the modification of the '404 reference would "increase the security of the system" relative to the unmodified '404 reference which already disguises the actual power consumed by the data carrier during security-relevant operations using complementary logic to achieve a constant power consumption. Nothing in the Patterson reference overcomes the deficiencies of the combination of the '404 reference, the '159 reference and the AAPA. As such, the Examiner's proposed modification involves adding redundant circuitry to the '404 reference without any perceived benefit.

VIII. Conclusion

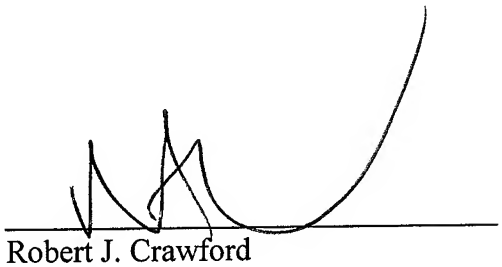
In view of the above, Appellant submits that the rejections of claims 1-8 and 10-14 are improper and therefore requests reversal of the rejections as applied to the appealed claims and allowance of the entire application.

Authority to charge the undersigned's deposit account was provided on the first page of this brief.

Please direct all correspondence to:

Corporate Patent Counsel
NXP Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131

CUSTOMER NO. 65913

By: 

Robert J. Crawford
Reg. No.: 32,122
Eric J. Curtin
Reg. No.: 47,511
651-686-6633
(NXPS.589PA)

APPENDIX OF CLAIMS INVOLVED IN THE APPEAL
(S/N 10/553,790)

1. An electronic circuit device for executing operations dependent on secret information, the electronic circuit device, comprising:

power supply connections;

a processing unit comprising a plurality of processing circuits for use in execution of respective parts of the operations dependent on the secret information, the processing circuits being fed from the power supply connections;

an activity monitor circuit, coupled to receive pairs of processing signals, each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits, the activity monitor circuit being arranged to derive activity information from each pair of processing signals, the activity information indicative of whether each of the processing circuits generates a logic level transition, and to derive from the activity information a combined activity signal indicative of a sum of power supply currents that will be consumed by the processing circuits dependent on the processing signals;

a current drawing circuit connected to the power supply connections and controlled by the activity monitor circuit to draw a cloaking current controlled by the combined activity signal, so that power supply current variations dependent on the secret information are cloaked in a combination of the cloaking current and current drawn by the processing circuits.

2. An electronic circuit device according to Claim 1, wherein the processing unit comprises a clock circuit, combinatorial logic circuits and registers clocked by the clock circuit and connected between respective parts of the combinatorial logic circuits, the pairs of processing signals comprising pairs of input and output signals of the registers, the current drawing circuit being arranged to adjust a value of the cloaking current dependent on the activity of the registers at instants synchronized by the clock circuit.

3. An electronic circuit device according to Claim 2, organized as a pipe-line of successive parts of the combinatorial logic circuits, each pair of successive parts coupled via a respective one or respective ones of the registers, the electronic circuit_device, comprising:

a plurality of activity monitor circuits each coupled to receive pairs of input and output signals of the respective one or ones of the registers between a respective pair of successive parts of the combinatorial logic circuits, and to derive a combined activity signal from the pairs of input output signals;

a plurality of current drawing circuits connected to the power supply connections, each controlled by a respective one of the activity monitor circuits to draw a cloaking current controlled by combined activity signal derived by that respective one of the activity monitor circuits.

4. An electronic circuit device according to Claim 3, arranged to activate the current drawing circuits in selected clock cycles, when the corresponding pipe-line stages process secret information.

5. An electronic circuit device according to Claim 1, having a trigger input coupled to the current drawing circuit, arranged to enable drawing of the cloaking current only upon receiving a trigger signal that triggers or accompanies execution of a secret information dependent process in the electronic circuit device.

6. An electronic circuit device according to Claim 1, comprising a reference current pattern generator, the current drawing circuit being arranged to adjust the value of the cloaking current so that the combination of the cloaking current and current drawn by the processing circuits substantially equals a temporal reference current pattern generated by the reference current pattern generator.

7. A method of executing operations dependent on secret information in an electronic circuit, the method comprising:

supplying power supply current to processing circuits;

executing respective parts of operations that are dependent on the secret information using the processing circuits;

receiving pairs of processing signals coming into and out of respective ones of the processing circuits, each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits;

deriving activity information from each pair of processing signals, the activity information indicative of whether each of the processing circuits generates a logic level transition,

deriving from the activity information a combined activity signal indicative of a sum of power supply currents that will be consumed by the processing circuits dependent on the processing signals;

drawing a cloaking current controlled by the combined activity signal, and combining that cloaking current with current drawn by the processing circuits so that power supply current variations dependent on the secret information are cloaked in the combination of the cloaking current and current drawn by the processing circuits.

8. The method of claim 7, further comprising determining the cloaking current by subtracting the sum of power supply currents from a temporal reference current pattern.

10. The method of claim 7, wherein deriving activity information from each pair of processing signals includes generating respective currents proportional to a difference between the input signal and the output signal of each of the pairs of processing signals, and wherein the sum of power supply currents is a sum of the respective currents.

11. The electronic circuit device of claim 1, further comprising a plurality of activity monitor circuits each coupled to receive the input and output signals of one of the processing circuits.

12. The electronic circuit device of claim 1, wherein the activity monitor circuit is configured to generate respective currents proportional to a difference between the input

signal and the output signal of each of the pairs of processing signals, and wherein the sum of power supply currents is a sum of the respective currents.

13. The electronic circuit device of claim 1, wherein the current drawing circuit is a digital to analog converter that is configured to convert a digitally coded value into an analog power supply current that is equal to the cloaking current.

14. The electronic circuit device of claim 6, further comprising a subtractor that is configured to determine the cloaking current by subtracting the sum of power supply currents from the temporal reference current pattern generated by the reference current pattern generator.

APPENDIX OF EVIDENCE

Appellant is unaware of any evidence submitted in this application pursuant to 37 C.F.R. §§ 1.130, 1.131, and 1.132.

APPENDIX OF RELATED PROCEEDINGS

As stated in Section II above, Appellant is unaware of any related appeals, interferences or judicial proceedings.